Information Commissioner's Office

Findings from ICO Information Risk Reviews on Information Security Breach Reporting in Central Government

December 2018

Introduction

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, and taking appropriate action where the law is broken.

In September 2016 the National Audit Office (NAO) published its report 'Protecting Information Across Government'. This emphasised the importance of protecting government information from unauthorised access or loss. It also highlighted many of the challenges and competing responsibilities that government departments face in this area.

Our concerns

The ICO was concerned by a section of the NAO's report that dealt with how departments handled the reporting of information security (IS) breaches. The NAO said it was "chaotic, with different mechanisms making departmental comparisons meaningless".

The NAO also said that the information given in the departments' annual reports about data incidents reported to the ICO did not match the ICO's own records.

Why we took action

At the time of the report, data controllers had no statutory duty (subject to some exceptions) to report data security incidents or similar contraventions involving personal data to the ICO.

However, the General Data Protection Regulation (GDPR) was on the horizon; this would require data controllers to notify the ICO of certain personal data breaches without undue delay and not later than 72 hours after they became aware of the breach.

With this in mind, we began a project to find out more about how central government departments manage their IS breach reporting.

We invited the 16 largest central government departments to allow our Assurance team to do targeted information risk reviews of their processes for data incident management and reporting.

Our aims were to:
• better understand these processes;
• clarify the problems identified in the NAO report; and
• examine any inconsistencies in the processes.

Our reviews: method, feedback and timing

We undertook desk-based reviews of breach-reporting policies and procedures, followed by short site visits and interviews with key staff to observe procedures in practice.

After each visit, we gave the department a short report on our findings and any areas of good practice or weakness we had identified. Where there were weaknesses, we made recommendations.

The site visits took place from February 2017 to May 2018.

This report gives an overview of the main themes that we identified through these reviews.

Which departments took part

The following departments agreed to take part:

The Cabinet Office
Department for Business, Energy & Industrial Strategy
Department for Communities and Local Government
Department for Culture, Media & Sport
Department for Environment, Food & Rural Affairs
Department for Education
Department for International Development
Department for Transport
Department of Health
Foreign & Commonwealth Office
HM Treasury
HM Revenue & Customs
Home Office
Ministry of Defence

Ministry of Justice

The Department for Work & Pensions also consented to an information risk review; however, we did not do a full review as a new incident management system was being rolled out at the time of the visit. Instead we reviewed the department's plans and gave comments.

Control areas

Our information risk reviews focused on the following control areas:

- **Responsibilities and procedures** – Management responsibilities and procedures should ensure a quick, effective and orderly response to IS incidents.

- **Awareness of information security events** – Staff should be aware of the nature of an IS event, its potential harm to the organisation and how to report it.

- **Reporting information security weaknesses** – Employees and contractors using the organisation's information systems and services should be required to note and report any observed or suspected IS weakness in systems or services.

- **Assessment of and decisions on information security events** – IS events should be assessed. It should be decided whether or not they are to be classed as IS incidents.

- **Response to information security incidents** – IS incidents should be responded to in line with the documented procedures.

- **Learning from information security incidents** – knowledge gained from analysing and resolving IS incidents should be used to reduce the likelihood or impact of future incidents.

Areas of good practice

We listed areas of good practice we identified during our information risk reviews. These examples were not consistent across all 16 government departments but were found in at least one department.

- **Staff are encouraged to report near misses**
    - 44% of departments encouraged staff to report near misses.

- **Use of reporting software to track incidents and responses**

    - 19% of departments used incident reporting software.

- **Yearly training and awareness plans include information security campaigns.**
    - 19% of departments had annual IS training and awareness campaigns.

- **Incident trends feed into Information Assurance Risk Registers**
    - 31% of departments tracked incident trends to inform their Information Assurance Risk Register.

- **ISO 27001 accreditation**
    - 13% of departments had ISO 27001 accreditation.

Areas for improvement

Based on the weaknesses we found, we made several recommendations to improve departmental breach-reporting processes. Again, the weaknesses were not consistent across all 16 government departments. We have grouped our recommendations under several headings:

Lack of staff awareness
In 75% of departments, staff lacked awareness about the processes for reporting and managing IS incidents. In particular, we identified failure to check whether policies had been read and understood; out-of-date or inaccurate guidance documents; failure to test staff knowledge of incident management processes; and a lack of communication of lessons learned from previous incidents.

Recommendation: Departments should regularly check to ensure that

Reliance on generic Civil Service e-learning
81% of departments relied on generic Civil Service e-learning as the sole source of information governance training. This resulted in a risk that training was not enough to meet specific team or departmental needs.

Recommendation: Generic training does not meet all needs, so departments should carry out regular training-needs analysis to identify what training individuals or teams require. This would help to ensure that those who have particular responsibilities or do particular types of work that involve unique or unusual issues do not face a greater risk of incidents/breaches.

Lack of role-specific training

50% of departments lacked role-specific training for job roles that:

- carry specific duties and responsibilities under data protection legislation;
- involve handling large volumes of personal data; or
- undertake particularly high-risk processing.

This shortcoming applies, for example, to positions like Data Protection Officer (DPO), Senior Information Risk Officer (SIRO), Information Asset Owner (IAO), and information request handlers.

Recommendation: Departments should do training-needs analysis to identify job roles that would benefit from specific, specialised training, then source and provide it.

Lack of follow-up of training completion

50% of departments had no process to ensure that staff had completed their training satisfactorily, or that they had been brought up to date on changes to key policies or procedures.

Recommendation: Processes should be put in place:

- to ensure that all staff have completed their information-governance training; and
- to track whether staff have been brought up to date on changes to policies and procedures.

These processes could include checklists for new starters or signed receipts to confirm that staff have read and understood new or amended policies and procedures.

Lack of central oversight

38% of departments had no system to allow central oversight of IS incidents. Such incidents were being managed locally without any requirement for onward reporting or escalation.

Recommendation: Where there is no central function for the reporting and management of IS incidents, processes should be in place to ensure that there is sufficient oversight of such incidents. This is important to:

- ensure consistency in how these incidents are investigated and resolved at a local level; and

• enable the department to analyse trends, which allows it to identify and tackle wider issues and themes.

Lack of definitions for classifying and escalating information security incidents
50% of departments lacked a process for classifying the seriousness of these incidents. This reduced their ability to respond to them, resolve them and learn from them in the most appropriate and effective way.

Recommendation: Incident management processes should include a means of classifying IS incidents according to their severity and seriousness. This would help departments be consistent in how they respond to, resolve and learn from incidents. It would also enable them to more quickly identify and escalate incidents that meet certain criteria.

Lack of defined roles and responsibility
56% of departments had no or poorly defined roles and responsibilities on managing IS incidents. Responsibilities were often informally assigned. They were not included in job descriptions or formally assigned in policies and procedures.

Recommendation: As regards managing IS incidents, departments should ensure that they:
• clearly define key roles and responsibilities;
• formally assign the key roles and responsibilities to specific individuals in relevant policies and procedures; and
• where possible, include the key roles and responsibilities in job descriptions or role profiles.
Once these roles and responsibilities are assigned, awareness-raising activities should occur to ensure all staff know who to contact for advice or assistance about IS incidents.

Lack of trend analysis and learning lessons
38% of departments did not carry out any trend analysis or exercises that would allow them to learn from IS incidents. This reduced their ability to identify weaknesses and risks. As a result, their risk registers didn't include relevant information governance risks that would have been identified through effective trend analysis.

Recommendation: Departments should put processes and procedures in place to allow them to identify, disseminate and learn lessons from IS incidents. These should involve finding the root causes and other contributing factors that might identify operational failures or weaknesses. Departments should then consider whether or not to escalate these findings and, where appropriate, add relevant risks to a risk register. They should also use this process to assess the effectiveness of how they manage such incidents and identify areas for improvement.

Recommendation: Departments should put processes in place that require regular trend analysis of IS incidents. Incident logs and investigation reports should be reviewed to identify any patterns that might indicate organisational weaknesses, such as gaps in training provision or lack of IS controls. The results of these exercises should be reported and escalated appropriately, to allow management to take any necessary remedial action.

Resources

The ICO has produced guidance for organisations to read on information security. See our website www.ico.org.uk

- Guide to GDPR
- Information Security Checklist
- Guidance on personal data breaches
- Notification of data security breaches to the ICO
- Data protection breach notification form